What is claimed is

1. A method for encrypting data according to an asymmetrical method, based on a factorization problem, having a public key and a private key; the public key being the iteration number L as well as the composite number n, n preferably being the product of a plurality of large prime numbers; the private key being made up of the factorization of n; the message $m = (m_1, m_2)$ to be encrypted being made up of at least the components m_1 *and* m_2; an encryption function $f(x)$ being iterated a total of L times, with $c=(c_1,c_2)=f^L(m)$; $f(m)=(f_1(m),f_2(m))$ being applicable, and $f_1=(m_1 op_1 m_2) \bmod n$ as well as $f_2=(m_1, op_2 m_2) \bmod n$; op_1 preferably being an addition and op_2 preferably being a multiplication; the encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the L-fold solution of a quadratic equation modulo n, it thereby being possible to retrieve the original message from the encrypted information $c = (c1, c2)$.

2. The method as recited in Claim 1,
wherein a multivaluedness of the quadratic equation is eliminated by additional bits of a_i und b_i.

3. The method as recited in Claim 2,
wherein the multivaluedness of the quadratic equation is eliminated by calculating a parity and a Jacobi symbol which, particularly in the case of prime numbers of form 3 mod 4, can be communicated by 2 bits per iteration step.

4. The method as recited in one or more of the preceding claims,
wherein general iterations $f_1=(k_1 \bullet m_1+k_2 \bullet m_2) \bmod n$ as well as $f_2=k_3 \bullet m_1 \bullet m_2 \bmod n$ are used, the constants being part of the public key.

5. The method as recited in one or more of the preceding claims,
wherein the composite number n as public key contains more than two factors.

6. The method as recited in one or more of the preceding claims,
wherein the message is now made up of an N-tuple $m=(m_1...m_N)$, the formula for the Lth iteration step using dependencies of N values in each iteration step.

7. The method as recited in Claim 6,
wherein the multivaluedness is resolved by additional bits that are derived from the values obtained in each iteration.

8. The method as recited in one or more of the preceding claims,
wherein the multivaluedness is resolved by redundancy in the transmitted data.

9. A method for generating a signature,
wherein a signature is generated by interchanging the encryption and decryption steps from the preceding method.

10. Software for a computer,
wherein a method as recited in one or more of the preceding claims is implemented.

11. A data carrier for a computer,
characterized by the storage of a software as recited in the preceding software claim.

12. A computer system,
characterized by a device that allows the execution of a method as recited in one or more of the preceding method claims.